US009419983B2

(12) United States Patent
Struik

(10) **Patent No.:** **US 9,419,983 B2**
(45) **Date of Patent:** ***Aug. 16, 2016**

(54) **METHOD AND APPARATUS FOR PROVIDING AN ADAPTABLE SECURITY LEVEL IN AN ELECTRONIC COMMUNICATION**

(71) Applicant: **Certicom Corp.**, Mississauga (CA)

(72) Inventor: **Marinus Struik**, Toronto (CA)

(73) Assignee: **Certicom Corp.**, Mississauga, ON (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/877,072**

(22) Filed: **Oct. 7, 2015**

(65) **Prior Publication Data**

US 2016/0028740 A1 Jan. 28, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/477,637, filed on Sep. 4, 2014, now Pat. No. 9,191,395, which is a continuation of application No. 10/885,115, filed on Jul. 7, 2004, now Pat. No. 8,862,866.

(60) Provisional application No. 60/484,656, filed on Jul. 7, 2003.

(51) **Int. Cl.**
H04L 29/06	(2006.01)
H04L 9/08	(2006.01)
H04L 9/00	(2006.01)
H04W 12/02	(2009.01)

(52) **U.S. Cl.**
CPC *H04L 63/105* (2013.01); *H04L 9/088* (2013.01); *H04L 63/08* (2013.01); *H04L*

63/123 (2013.01); *H04L 63/164* (2013.01); *H04L 9/00* (2013.01); *H04W 12/02* (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/08; H04L 63/123; H04L 63/164; H04L 63/105; H04L 9/00; H04L 9/088; H04W 12/02
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,099,517 A	3/1992	Gupta et al.
5,301,287 A	4/1994	Herrell et al.
5,450,493 A	9/1995	Maher
5,638,448 A	6/1997	Nguyen
5,689,566 A	11/1997	Nguyen

(Continued)

FOREIGN PATENT DOCUMENTS

EP	1320010	6/2003
EP	1324541	7/2003

(Continued)

OTHER PUBLICATIONS

Kent, Stephen T. "Internet privacy enhanced mail." Communications of the ACM 36.8 (1993): 48-60.*

(Continued)

Primary Examiner — Kari Schmidt
(74) *Attorney, Agent, or Firm* — Fish & Richardson P.C.

(57) **ABSTRACT**

A method of communicating in a secure communication system, comprises the steps of assembling a message at a sender, then determining a security level, and including an indication of the security level in a header of the message. The message is then sent to a recipient.

21 Claims, 3 Drawing Sheets
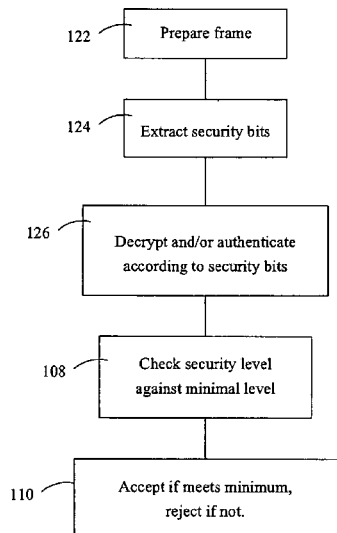
(56) **References Cited**

U.S. PATENT DOCUMENTS

5,832,228	A	11/1998	Holden et al.
6,044,062	A	3/2000	Brownrigg
6,101,543	A	8/2000	Alden et al.
6,108,583	A	8/2000	Schneck et al.
6,118,775	A	9/2000	Kari et al.
6,272,632	B1	8/2001	Carman et al.
6,510,349	B1	1/2003	Schneck et al.
6,760,768	B2	7/2004	Holden et al.
6,782,473	B1	8/2004	Park
6,792,111	B1	9/2004	Italia
6,865,426	B1	3/2005	Schneck et al.
6,918,034	B1	7/2005	Sengodan et al.
6,928,544	B2	8/2005	Chu
7,016,948	B1	3/2006	Yildiz
7,023,863	B1	4/2006	Naudus et al.
7,024,609	B2	4/2006	Wolfgang et al.
7,031,309	B1	4/2006	Sautter
7,036,015	B2	4/2006	Vanstone et al.
7,107,335	B1	9/2006	Arcieri et al.
7,143,137	B2	11/2006	Maufer et al.
7,233,948	B1	6/2007	Shamoon et al.
7,302,564	B2	11/2007	Berlin
7,412,726	B1	8/2008	Viswanath
7,437,548	B1	10/2008	Alfieri
7,447,313	B2	11/2008	Van Rijnsoever
7,467,406	B2	12/2008	Cox et al.
7,526,807	B2	4/2009	Chao et al.
7,600,038	B2	10/2009	Struik
7,657,531	B2	2/2010	Bisbee et al.
7,660,986	B1	2/2010	Qiu et al.
7,965,843	B1	6/2011	Maino et al.
8,069,483	B1	11/2011	Matlock
2001/0043577	A1	11/2001	Barany et al.
2002/0035635	A1	3/2002	Holden et al.
2002/0090086	A1	7/2002	Van Rijnsoever
2002/0174352	A1	11/2002	Dahl
2002/0176433	A1	11/2002	Zhu et al.
2002/0181493	A1	12/2002	Bamba
2003/0012163	A1	1/2003	Cafarelli
2003/0026255	A1	2/2003	Poeluev et al.
2003/0035542	A1	2/2003	Kim
2003/0119484	A1	6/2003	Adachi et al.
2003/0156586	A1	8/2003	Lee
2003/0159036	A1	8/2003	Walmsley et al.
2003/0226011	A1	12/2003	Kuwano et al.
2004/0010691	A1	1/2004	Nelson
2004/0028409	A1	2/2004	Kim et al.
2004/0047324	A1	3/2004	Diener
2004/0062224	A1	4/2004	Brownrigg
2004/0136527	A1	7/2004	Struik
2004/0139312	A1	7/2004	Medvinsky
2004/0218683	A1	11/2004	Batra
2004/0223615	A1*	11/2004	Dhawan H04K 1/04
			380/261
2004/0255001	A1	12/2004	Oh et al.
2005/0015583	A1	1/2005	Sarkkinen et al.
2005/0076197	A1	4/2005	Struik
2005/0081032	A1	4/2005	Struik
2005/0086501	A1	4/2005	Woo et al.
2005/0108746	A1	5/2005	Futagami et al.
2006/0050708	A1	3/2006	Shapiro
2006/0064736	A1	3/2006	Ahuja et al.
2006/0075480	A1	4/2006	Noehring
2006/0112431	A1	5/2006	Finn et al.
2006/0140400	A1	6/2006	Brown et al.
2006/0210071	A1	9/2006	Chandran et al.
2007/0058633	A1	3/2007	Chen et al.
2007/0086397	A1	4/2007	Taylor
2007/0160059	A1	7/2007	Poeluev et al.
2007/0195788	A1	8/2007	Vasamsetti et al.
2007/0255954	A1	11/2007	Struik
2008/0177997	A1	7/2008	Morais et al.
2008/0307524	A1	12/2008	Singh et al.
2009/0290635	A1	11/2009	Kim
2009/0319775	A1	12/2009	Buer et al.

2011/0106956	A1	5/2011	Luo
2011/0209196	A1*	8/2011	Kennedy G06F 21/55
			726/1
2011/0264915	A1	10/2011	Cam-Winget et al.

FOREIGN PATENT DOCUMENTS

EP	1326157	7/2003
WO	00/10304	2/2000
WO	03/036857	5/2003
WO	2005/083970	9/2005

OTHER PUBLICATIONS

Li, Renqi, and E. A. Unger. "Security issues with TCP/IP." ACM SIGAPP Applied Computing Review 3.1 (1995): 6-13.*

LeMay, Michael D., and Jack SE Tan. "Comprehensive message control and assurance with the secure email transport protocol." Electro/Information Technology Conference, 2004. EIT 2004. IEEE. IEEE, 2004.*

Cam-Winget et al. "Security Flaws in 802.11 Data Link Protocols" Communications of the ACM 46.5 (May 2003) pp. 35-39.

Dierks, T. et al.; "The TLS Protocol"; RFC 2246; IETF; Jan. 1999; pp. 23, 28-30.

Hura et al.; "Data and Computer Communications: Networking and Internetworking"; CRC Press, 2001; pp. 337, 450, 453, 467, 471, 483, 484, 485, 489, 491, 526, 599, 609, 617, 618, 621, 937, 1086, 1117, 1118, 1132.

IEEE Standard 802.11; Standard for Telecommunications and Information Exchange between Systems—Local and Metropolitan Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; IEEE Press; 1999; pp. 34-41, 50-58.

Kent, S. et al.; "IP Authentication Header"; RFC 2402; IETF; Nov. 1998; 21 pages.

Kent, S. et al.; "Security Architecture for the Internet Protocol"; RFC 2401; IETF; Nov. 1998; 62 pages.

Oppliger; "Security at the Internet Layer" Computer 31.9 (1998) pp. 43-47.

Specification of the Bluetooth System; Specification vol. 1—Core, Version 1.0B; Dec. 1, 1999; p. 160.

Sung et al.; "Design and Evaluation of Adaptive Secure Protocol for E-Commerce"; Proceedings of the 10th International Conference on Computer Communications and Networks; Oct. 15-17, 2001; pp. 32-39.

"Transmission Control Protocol"; RFC 0793; Darpa Internet Program; Information Sciences Institute; University of Southern California; Sep. 1981.

Office Action issued in U.S. Appl. No. 10/921,161 on Mar. 25, 2008; 24 pages.

Office Action issued in U.S. Appl. No. 10/921,161 on Nov. 25, 2008; 30 pages.

Office Action issued in U.S. Appl. No. 10/921,161 on Dec. 9, 2009; 25 pages.

Office Action issued in U.S. Appl. No. 10/921,161 on Aug. 18, 2010; 27 pages.

Office Action issued in U.S. Appl. No. 10/921,161 on Jan. 27, 2011; 30 pages.

Examiner's Answer to Appeal Brief issued in U.S. Appl. No. 10/921,161 on Feb. 21, 2012; 30 pages.

Notice of Allowance issued in U.S. Appl. No. 10/921,161 on Apr. 12, 2012; 9 pages.

Office Action issued in U.S. Appl. No. 13/551,869 on Apr. 2, 2013; 11 pages.

Notice of Allowance issued in U.S. Appl. No. 13/551,869 on Sep. 27, 2013; 9 pages.

Office Action issued in U.S. Appl. No. 11/735,055 on Jul. 13, 2010; 21 pages.

Office Action issued in U.S. Appl. No. 11/735,055 on Dec. 22, 2010; 14 pages.

Office Action issued in U.S. Appl. No. 11/735,055 on Feb. 17, 2012; 14 pages.

(56)   **References Cited**

OTHER PUBLICATIONS

Office Action issued in U.S. Appl. No. 11/735,055 on Dec. 11, 2012; 15 pages.
Office Action issued in U.S. Appl. No. 11/735,055 on May 24, 2013; 16 pages.
Notice of Allowance issued in U.S. Appl. No. 11/735,055 on Nov. 25, 2013; 23 pages.
Office Action issued in Canadian Application No. 2,434,992 on Sep. 14, 2011; 3 pages.
Office Action issued in Canadian Application No. 2,434,992 on Dec. 5, 2012; 2 pages.
Notice of Allowance issued in Canadian Application No. 2,434,992 on Dec. 9, 2013; 1 page.
Office Action issued in Canadian Application No. 2,478,274 on Feb. 3, 2012; 2 pages.
Office Action issued in Canadian Application No. 2,478,274 on Mar. 14, 2013; 3 pages.
Office Action issued in Canadian Application No. 2,478,274 on Jan. 7, 2014; 2 pages.
Office Action issued in Canadian Application No. 2,644,015 on May 23, 2012; 3 pages.
Office Action issued in Canadian Application No. 2,644,015 on Nov. 4, 2013; 4 pages.
Office Action issued in Chinese Application No. 200780020042.X on Jan. 14, 2004; 10 pages.
Office Action issued in Chinese Application No. 200780020042.X on Mar. 21, 2012; 10 pages.
Office Action issued in Chinese Application No. 200780020042.X on Aug. 13, 2012; 9 pages.
Office Action issued in Chinese Application No. 200780020042.X on Dec. 17, 2012; 7 pages.
Notice of Allowance issued in Chinese Application No. 200780020042.X on May 6, 2013; 4 pages.

Search Report issued in U.K. Application No. 0418565.8 on Jan. 25, 2005; 4 pages.
Examination Report issued in U.K. Application No. 0418565.8 on Oct. 31, 2005; 7 pages.
Examination Report issued in U.K. Application No. 0418565.8 on Feb. 15, 2006; 2 pages.
Examination Report issued in U.K. Application No. 0418565.8 on Aug. 23, 2006; 3 pages.
Combined Search and Examination Report issued in U.K. Application No. 0623685.5 on Mar. 16, 2007; 5 pages.
Combined Search and Examination Report issued in U.K. Application No. 0721922.3 on Dec. 18, 2007; 5 pages.
Examination Report issued in German Application No. 102004040312.0 on Oct. 24, 2012; 15 pages.
Extended European Search Report issued in European Patent Application No. 07719535.2 on May 13, 2011; 6 pages.
Communication Pursuant to Article 94(4) EPC issued in European Application No. 07719535.2 on Feb. 17, 2012; 5 pages.
Communication Pursuant to Article 94(4) EPC issued in European Application No. 07719535.2 on Mar. 8, 2013; 5 pages.
Communication Pursuant to Article 94(4) EPC issued in European Application No. 07719535.2 on Feb. 7, 2014; 7 pages.
Official Action issued in Japanese Application No. 2009-504535 on Aug. 17, 2011; 9 pages.
Notice of Allowance issued in Japanese Application No. 2009-504535 on Dec. 13, 2011; 3 pages.
Notice of Allowance issued in Japanese Application No. 2011-251567 on Apr. 23, 2013; 3 pages.
Office Action issued in Korean Application No. 10-2008-7027745 on Jun. 28, 2013; 6 pages.
International Search Report and Written Opinion of the International Searching Authority issued in International Application No. PCT/CA2007/000608 on Aug. 28, 2007; 4 pages.
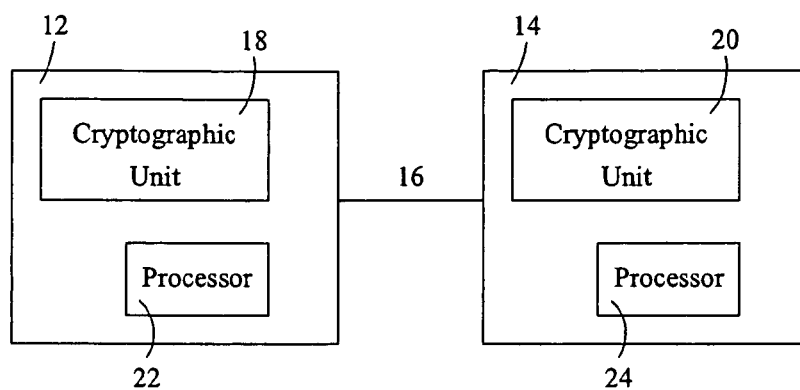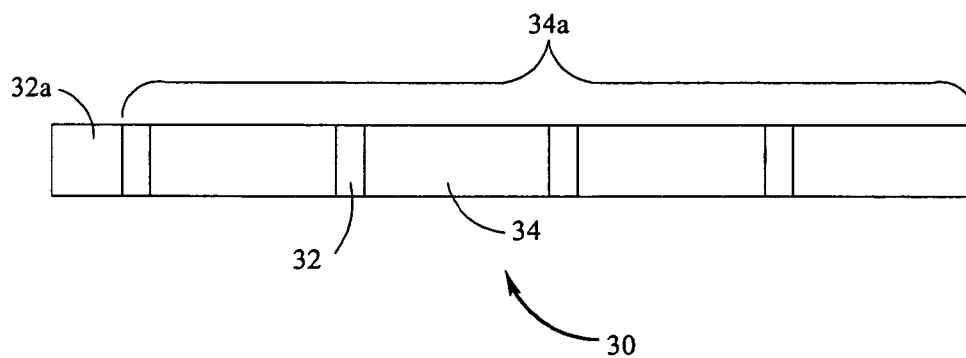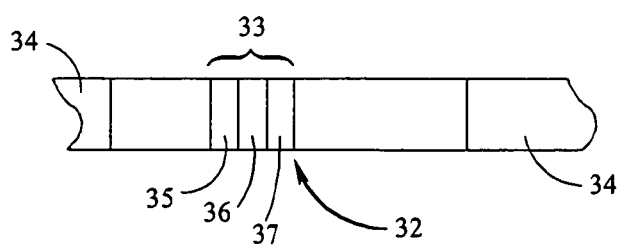SunScreen 3.2 Administrators Overview, Sep. 2001, pp. 1-356.

* cited by examiner

12
18
Cryptographic Unit

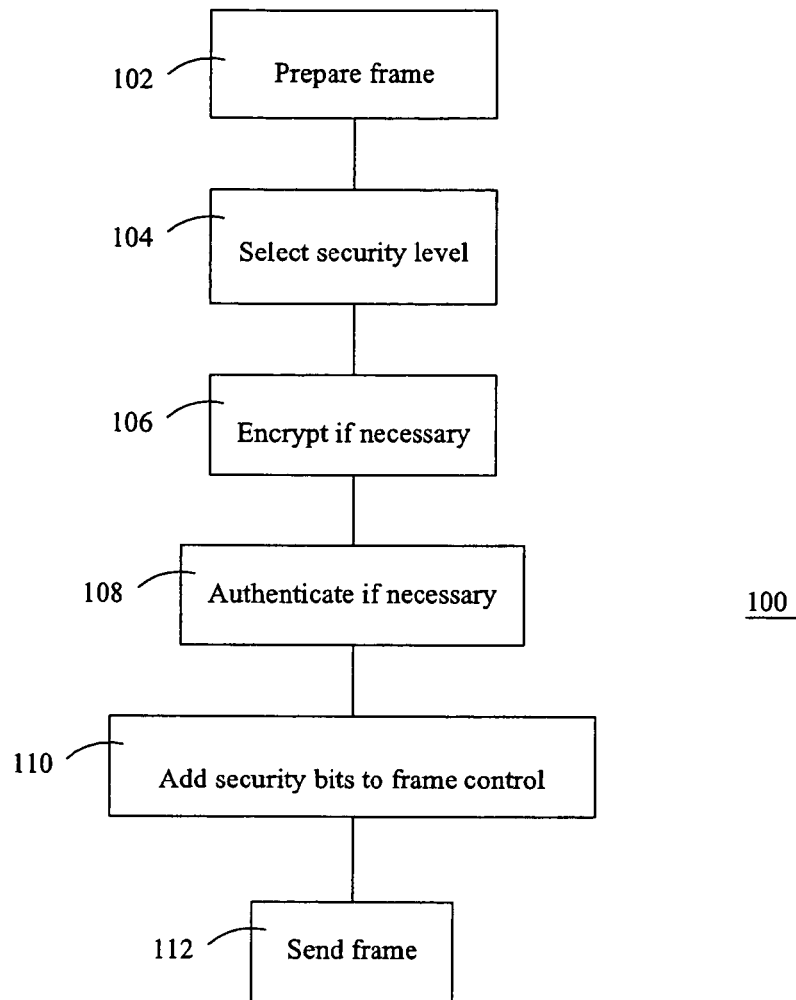Processor

22

16

14
20
Cryptographic Unit

Processor

24

Figure 1

34a

32a

32

34

30

Figure 2

34

33

35 36 37 32

34

Figure 3

Figure 4

122 — Prepare frame

124 — Extract security bits

126 — Decrypt and/or authenticate according to security bits

108 — Check security level against minimal level
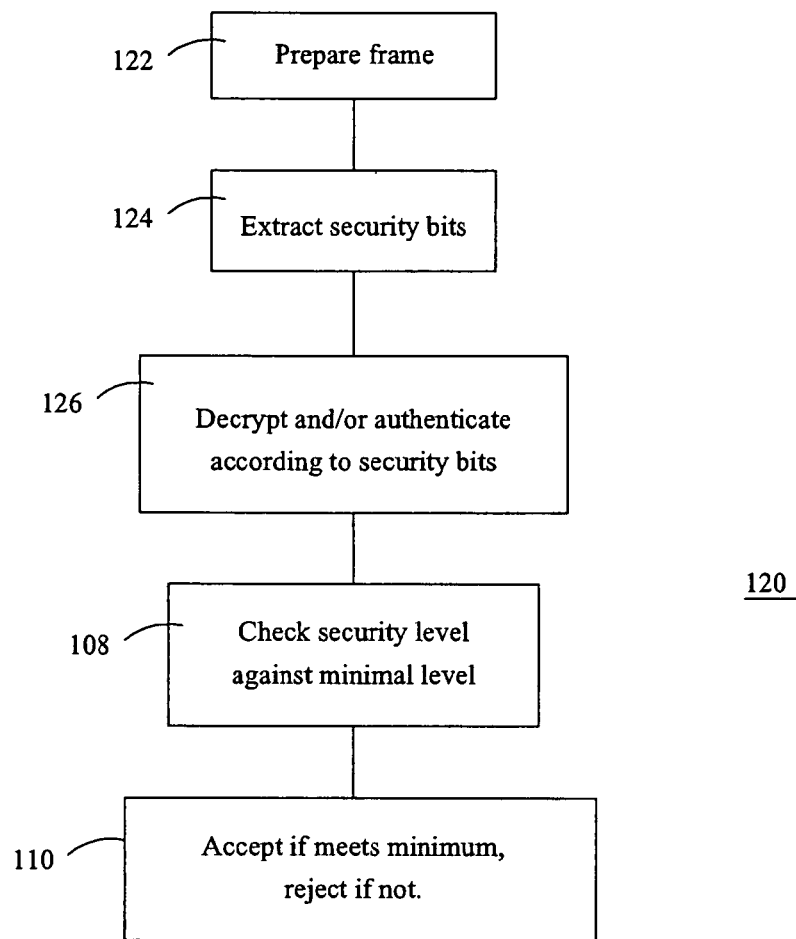
110 — Accept if meets minimum, reject if not.

120

Figure 5

METHOD AND APPARATUS FOR PROVIDING AN ADAPTABLE SECURITY LEVEL IN AN ELECTRONIC COMMUNICATION

This application is a continuation of and claims priority to U.S. application Ser. No. 14/477,637, filed on Sep. 4, 2014, which is a continuation of and claims priority to U.S. application Ser. No. 10/885,115, filed on Jul. 7, 2004, now U.S. Pat. No. 8,862,866, which claims priority from U.S. Provisional Patent Application No. 60/484,656 filed on Jul. 7, 2003. The entire contents of which is hereby incorporated by reference for all purposes.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a method and apparatus for providing an adaptable security level in an electronic communication.

2. Description of the Prior Art

In electronic communications, it is often necessary to prevent an eavesdropper from intercepting message. It is also desirable to have an indication of the authenticity of a message, that is a verifiable identification of the sender. These goals are usually achieved through the use of cryptography. Private key cryptography requires sharing a secret key prior to initiating communications. Public key cryptography is generally preferred as it does not require such a shared secret key. Instead, each correspondent has a key pair including a private key and a public key. The public key may be provided by any convenient means, and does not need to be kept secret.

There are many variations in cryptographic algorithms, and various parameters that determine the precise implementation. In standards for wireless communications, it has been customary to set these parameters in advance for each frame type. However, this approach limits the flexibility of the parameters.

When one device is communicating with several other devices, it will often need to establish separate parameters for each communication.

It is an object of the present invention to obviate or mitigate the above disadvantages.

SUMMARY OF THE INVENTION

In accordance with one aspect of the present invention, there is provided a method of communicating in a secure communication system, comprising the steps of assembling as message at a sender, then determining a security level, and including an indication of the security level in a header of the message. The message is then sent to a recipient.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

FIG. 1 is a schematic representation of a communication system;

FIG. 2 is a schematic representation of an information frame exchanged in the communication system of FIG. 1;

FIG. 3 is a schematic representation of a frame control portion of the frame of FIG. 2;

FIG. 4 is a schematic representation of a method performed by a sender in FIG. 1;

FIG. 5 is a schematic representation of a method performed by a recipient in FIG. 1.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring to FIG. 1, a communication system 10 includes a pair of correspondents 12, 14 connected by a communication link 16. Each correspondent 12, 14 includes a respective cryptographic unit 18, 20.

Each correspondent 12, 14 can include a processor 22, 24. Each processor may be coupled to a display and to user input devices, such as a keyboard, mouse, or other suitable devices. If the display is touch sensitive, then the display itself can be employed as the user input device. A computer readable storage medium is coupled to each processor 22, 24 for providing instructions to the processor 22, 24 to instruct and/or configure processor 22, 24 to perform steps or algorithms related to the operation of each correspondent 12, 14, as further explained below. The computer readable medium can include hardware and/or software such as, by way of example only, magnetic disks, magnetic tape, optically readable medium such as CD ROM's, and semi-conductor memory such as PCMCIA cards. In each case, the medium may take the form of a portable item such as a small disk, floppy diskette, cassette, or it may take the form of a relatively large or immobile item such as hard disk drive, solid state memory card, or RAM provided in a support system. It should be noted that the above listed example mediums can be used either alone or in combination.

In order to transfer data between the correspondents 12, 14, a packet stream 30 is assembled at one of the correspondents in accordance with a defined protocol. The packet stream 30 is shown schematically in FIG. 2 and is composed of one or more frames 31, each of which has a header 32 and data 34. In some protocols, the packet may itself be organised as a frame with a header 32a and the data 34a consisting of a collection of individual frames. The header 32 is made up of a string of bits and contains control information at specified locations within the bit stream.

Included in each of the headers 34 are security control bits 33, that included a security mode bit 35 and integrity level bits 36,37.

In this embodiment, security bit mode 35 is used to indicate whether encryption is on or off. Security bits 36 and 37 together are used to indicate which of four integrity levels, such as 0, 32, 64, or 128 bit key size is utilised. The security mode bit may be used to indicate alternative modes of operation, such as, authentication and the number of bits may be increased to accommodate different combinations. It will be recognized that providing security bits in each frame 31 of the stream 30 allows the security level to be on a frame-by-frame basis rather than on the basis of a pair of correspondents, therefore providing greater flexibility in organizing communications.

In order to provide security, certain minimum security levels may be used. These levels should be decided upon among all of the correspondents through an agreed-upon rule. This rule may be either static or dynamic.

In operation, the correspondent 12 performs the steps shown in FIG. 4 by the numeral 100 to send information to the correspondent 14. First, the correspondent 12 prepares data and a header at step 102. Then it selects the security level at step 104. The security level is determined by considering the minimum security level required by the recipient, the nature of the recipient, and the kind of data being transmitted. If the security level includes encryption, then the correspondent 12

encrypts the data at step **106**. If the security level includes authentication, then the correspondent **12** signs the data at step **108**. Then the correspondent **12** includes bits indicating the security mode and security level in the frame control at step **110**. The correspondent **12** then sends the frame to the correspondent **14**.

Upon receiving the frame, the correspondent **14** performs the steps shown in FIG. **5** by the numeral **120**. The correspondent **14** first receives the frame at step **122**. It then extracts the security bits at step **124**. If the mode security bits **34** indicate encryption, then the correspondent **14** decrypts the data at step **126**. If the security bits indicate authentication, then the correspondent **14** verifies the signature at step **126**. Finally, the correspondent **14** checks the security level to ensure it meets predetermined minimum requirements. If either the encryption or authentication fails, or if the security level does not meet the minimum requirements, then the correspondent **14** rejects the message.

It will be recognized that providing security bits and an adjustable security level provides flexibility in protecting each frame of the communication. It is therefore possible for the sender to decide which frames should be encrypted but not authenticated. Since authentication typically increases the length of a message, this provides a savings in constrained environments when bandwidth is at a premium.

In a further embodiment, the correspondent **12** wishes to send the same message to multiple recipients **14** with varying minimum security requirements. In this case, the correspondent **12** chooses a security level high enough to meet all of the requirements. The correspondent **12** then proceeds as in FIG. **4** to assemble and send a message with the security level. The message will be accepted by each recipient since it meets each of their minimum requirements. It will be recognized that this embodiment provides greater efficiency than separately dealing with each recipient's requirements.

In another embodiment, a different number of security bits are used. The actual number of bits is not limited to any one value, but rather may be predetermined for any given application. The security bits should indicate the algorithm parameters. They may be used to determine the length of a key as 40 bits or 128 bits, the version of a key to be used, or any other parameters of the encryption system.

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follow:

1. A method performed by a communication device, the method comprising:

said communication device receiving a plurality of frames, wherein each individual frame having a header and associated data, the header of each individual frame including security control bits that indicate for that individual frame whether encryption has been provided for the individual frame and whether integrity has been provided for the individual frame, wherein the security control bits include one or more security mode bits and integrity level bits, wherein the one or more security mode bits are used to indicate whether encryption is on or off, and wherein the integrity level bits indicate which of at least four integrity levels is utilized, the integrity levels corresponding to signing operations of a sender of increasing strength;

on a frame-by-frame basis, for each individual frame, said communication device:

identifying a security level for the individual frame based on the security control bits in the header of the frame;

checking said security level against predetermined minimum security requirements for said communication device; and

rejecting the individual frame in response to said security level not meeting said predetermined minimum security requirements.

2. The method according to claim **1**, wherein said security level is selected by another device based on said predetermined security requirements for said communication device.

3. The method according to claim **2**, wherein said predetermined security requirements are determined among said communication device and said other device based on an agreed-upon rule.

4. The method according to claim **1**, wherein said security control bits include an indication of a cryptographic algorithm parameter.

5. The method according to claim **1**, further comprising decrypting each frame according to said security level for the frame.

6. The method according to claim **1**, further comprising verifying the integrity of each frame according to said security level for the frame.

7. The method of claim **1**, wherein the number of integrity levels is four, and the four integrity levels correspond to key lengths of 0, 32, 64, and 128 bits.

8. The method of claim **1**, wherein one of the integrity levels uses a key length of 128 bits.

9. The method of claim **1**, wherein one of the integrity levels indicates no integrity security.

10. The method of claim **1**, wherein the number of integrity levels is at least four, and the at least four levels include four levels corresponding to key lengths of 0, 32, 64, and 128 bits.

11. A non-transitory computer-readable storage medium comprising computer-executable instructions that are configured when executed, by data processing apparatus of a communication device, to perform operations comprising:

receiving a plurality of frames, wherein each individual frame having a header and associated data, the header of each individual frame including security control bits that indicate for that individual frame whether encryption has been provided for the individual frame and whether integrity has been provided for the individual frame, wherein the security control bits include one or more security mode bits and integrity level bits, wherein the one or more security mode bits are used to indicate whether encryption is on or off, and wherein the integrity level bits indicate which of at least four integrity levels is utilized, the integrity levels corresponding to signing operations of a sender of increasing strength;

on a frame-by-frame basis, for each individual frame:

identifying a security level for the individual frame based on the security control bits in the header of the frame;

checking said security level against predetermined minimum security requirements for said communication device; and

rejecting the individual frame in response to said security level not meeting said predetermined minimum security requirements.

12. The non-transitory computer-readable storage medium according to claim **11**, wherein said security level is selected by another device based on said predetermined security requirements for said communication device.

US 9,419,983 B2

5

13. The non-transitory computer-readable storage medium according to claim **11**, wherein said predetermined security requirements are determined among the communication device and another device based on an agreed-upon rule.

14. The non-transitory computer-readable storage medium according to claim **11**, wherein said security control bits include an indication of a cryptographic algorithm parameter.

15. The non-transitory computer-readable storage medium according to claim **11**, the operations further comprising decrypting each frame according to said security level for the frame.

16. The non-transitory computer-readable storage medium according to claim **11**, the operations further comprising verifying the integrity of each frame according to said security level for the frame.

17. The non-transitory computer-readable storage medium according to claim **11**, wherein the number of integrity levels is four, and the four integrity levels correspond to key lengths of 0, 32, 64, and 128 bits.

18. The non-transitory computer-readable storage medium according to claim **11**, wherein one of the integrity levels uses a key length of 128 bits.

19. The non-transitory computer-readable storage medium according to claim **11**, wherein one of the integrity levels indicates no integrity security.

20. The non-transitory computer-readable storage medium according to claim **11**, wherein the number of integrity levels is at least four, and the at least four levels include four levels corresponding to key lengths of 0, 32, 64, and 128 bits.

6

21. A device, comprising:
a memory; and
one or more processors communicatively coupled with the memory and configured to:
receive a plurality of frames, wherein each individual frame having a header and associated data, the header of each individual frame including security control bits that indicate for that individual frame whether encryption has been provided for the individual frame and whether integrity has been provided for the individual frame, wherein the security control bits include one or more security mode bits and integrity level bits, wherein the one or more security mode bits are used to indicate whether encryption is on or off, and wherein the integrity level bits indicate which of at least four integrity levels is utilized, the integrity levels corresponding to signing operations of a sender of increasing strength; and
on a frame-by-frame basis, for each individual frame:
identify a security level for the individual frame based on the security control bits in the header of the frame;
check said security level against predetermined minimum security requirements for said communication device; and
reject the individual frame in response to said security level not meeting said predetermined minimum security requirements.

* * * * *